GUIDANCE FOR A RISK-BASED APPROACH

THE BANKING SECTOR

OCTOBER 2014

FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

www.fatf-gafi.org

TABLE OF CONTENTS

TABLE OF ACRONYMS

AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
BCBS	Basel Committee on Banking Supervision
BCP	Basel Core Principle
CDD	Customer Due Diligence
DNFBP	Designated Non-Financial Business and Profession
FIU	Financial Intelligence Unit
INR []	Interpretive Note to Recommendation []
ML	Money Laundering
PEP	Politically Exposed Person
RBA	Risk-based approach
R. []	Recommendation []
TF	Terrorist Financing

RISK-BASED APPROACH GUIDANCE FOR THE BANKING SECTOR

This guidance paper should be read in conjunction with:

- the FATF Recommendations, especially Recommendations 1 and 26 (R. 1, R. 26) and their Interpretive Notes (INR), and the Glossary.
- other relevant FATF documents, such as the *FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment*, the *FATF Guidance on Politically Exposed Persons*, or the *FATF Guidance on AML/CFT and Financial Inclusion*.

INTRODUCTION

A. BACKGROUND AND CONTEXT

1. The risk-based approach (RBA) is central to the effective implementation of the revised FATF *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation*, which were adopted in 2012[1]. The FATF has reviewed its 2007 RBA guidance for the financial sector, in order to bring it in line with the new FATF requirements[2] and to reflect the experience gained by public authorities and the private sector over the years in applying the RBA. This revised version focuses on the banking sector[3], and a separate guidance will be developed for the securities sector. The FATF will also review its other RBA guidance papers, all based on the 2003 Recommendations[4].

2. The RBA guidance for the banking sector was drafted by a group of FATF members, co-led by the UK and Mexico[5]. Representatives of the private sector were associated to the work[6] and consulted on the draft revised document[7].

---

1 FATF (2012)

2 The FATF Standards are comprised of the FATF Recommendations, their Interpretive Notes and applicable definitions from the Glossary.

3 Banking activities are activities or operations described in the FATF Glossary under "Financial institutions", in particular 1., 2. and 5. The present guidance is intended for institutions providing these services.

4 Between June 2007 and October 2009, the FATF adopted a set of guidance papers on the application of the RBA for different business sectors: financial sector, real estate agents, accountants, trust and company service providers (TCSPs), dealers in precious metals and stones, casinos, legal professionals, money services businesses (MSBs) and the life insurance sector (www.fatf-gafi.org/documents/riskbasedapproach/).

5 The FATF Project group was composed of representatives from FATF members (Argentina; Australia; Austria; Belgium; Brazil; China; France; Germany; Hong Kong, China; India; Italy; Japan; Mexico; Spain; Switzerland; the Netherlands; the UK; the US), Associate members (Asia/Pacific Group on Money Laundering (APG) - through Bangladesh and Thailand and MONEYVAL - through Poland) and Observers (Basel Committee on Banking Supervision (BCBS), Organization for Security and Co-operation in Europe (OSCE), International Organisation of Securities Commissions (IOSCO), International Association of

3. The FATF adopted this updated RBA Guidance for the banking sector at its October 2014 Plenary.

B. PURPOSE OF THIS GUIDANCE

4. The purpose of this Guidance is to:

- Outline the principles involved in applying a risk-based approach to AML/CFT;
- Assist countries, competent authorities and banks in the design and implementation of a risk-based approach to AML/CFT by providing general guidelines and examples of current practice;
- Support the effective implementation and supervision of national AML/CFT measures, by focusing on risks and on mitigation measures; and
- Above all, support the development of a common understanding of what the risk-based approach to AML/CFT entails.

C. TARGET AUDIENCE, STATUS AND CONTENT OF THE GUIDANCE

5. This Guidance addresses countries and their competent authorities, including banking supervisors. It also addresses practitioners in the banking sector.

6. It consists of three sections. Section I sets out the key elements of the risk-based approach and needs to be read in conjunction with Sections II and III, which provide specific guidance on the effective implementation of a RBA to banking supervisors (Section II) and banks (Section III).

7. This Guidance recognises that an effective RBA will build on, and reflect, a country's legal and regulatory approach, the nature, diversity and maturity of its banking sector and its risk profile. It sets out what countries should consider when designing and implementing a RBA; but it does not override the purview of national competent authorities. When considering the general principles outlined in the Guidance, national authorities will have to take into consideration their national context, including the supervisory approach and legal framework.

Insurance Supervisors (IAIS), Group of International Finance Centre Supervisors (GIFCS), International Monetary Fund (IMF) and World Bank).

6 Amex, the Association of Development Financing Institutions in Asia and the Pacific (ADFIAP), the European Association of Co-operative Banks (EACB), the European Association of Public Banks (EAPB), the European Banking Federation (EBF), the European Banking Industry Committee (EBIC), the Latin American Banking Federation (FELABAN), the International Banking Federation (IBFed), SWIFT, the Banking Association of South Africa, the Wolfsberg Group, the Union of Arab Banks (UAB), the World Council of Credit Unions (WOCCU) and the World Savings Banks Institute/European Savings Banks Group (WSBI/ESBG) appointed representatives to the Project Group.

7 Comments were received from the Banking Association of South Africa, EBF, EBIC, EAPB, EACB, FELABAN, WOCCU, WSBI/ESBG, as well as from the International Council of Securities Association, the International Association of Money Transfer Networks, the International Consortium of Real Estate Associations, and the Russian e-money Association.

8. This guidance paper is non-binding. It draws on the experiences of countries and of the private sector and may assist competent authorities and financial institutions to effectively implement some of the Recommendations.

SECTION I – THE FATF'S RISK-BASED APPROACH (RBA) TO AML/CFT

A. WHAT IS THE RBA?

9. A RBA to AML/CFT means that countries, competent authorities and financial institutions[8], are expected to identify, assess and understand the ML/TF risks to which they are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively.

10. When assessing ML/TF risk[9], countries, competent authorities, and financial institutions should analyse and seek to understand how the ML/TF risks they identify affect them; the risk assessment therefore provides the basis for the risk-sensitive application of AML/CFT measures[10]. The RBA is not a "zero failure" approach; there may be occasions where an institution has taken all reasonable measures to identify and mitigate AML/CFT risks, but it is still used for ML or TF purposes.

11. A RBA does not exempt countries, competent authorities and financial institutions from mitigating ML/TF risks where these risks are assessed as low[11].

B. THE RATIONALE FOR A NEW APPROACH

12. In 2012, the FATF updated its Recommendations to strengthen global safeguards and to further protect the integrity of the financial system by providing governments with stronger tools to take action against financial crime.

13. One of the most important changes was the increased emphasis on the RBA to AML/CFT, especially in relation to preventive measures and supervision. Whereas the 2003 Recommendations provided for the application of a RBA in some areas, the 2012 Recommendations consider the RBA to be an 'essential foundation' of a country's AML/CFT framework.[12] This is an over-arching requirement applicable to all relevant FATF Recommendations.

14. According to the Introduction to the 40 Recommendations, the RBA 'allows countries, within the framework of the FATF requirements, to adopt a more flexible set of measures in order to target their resources more effectively and apply preventive measures that are commensurate to the nature of risks, in order to focus their efforts in the most effective way'.

---

8 Including both physical and natural persons, see definition of "Financial institutions" in the FATF Glossary.

9 FATF (2013a), *par.* 10.

10 FATF (2013a), *par.* 10. See also Section I D for further detail on identifying and assessing ML/TF risk.

11 Where the ML/TF risks have been assessed as low, INR 1 allows countries not to apply some of the FATF Recommendations, while INR 10 allows the application of Simplified Due Diligence measures to take into account the nature of the lower risk – see INR 1 para 6, 11 and 12 and INR 10 para 16 and 21.

12 R. 1.

15. The application of a RBA is therefore not optional, but a prerequisite for the effective implementation of the FATF Standards[13].

C. APPLICATION OF THE RISK-BASED APPROACH

16. Recommendation 1 sets out the scope of the application of the RBA. It applies in relation to:

- Who and what should be subject to a country's AML/CFT regime: in addition to the sectors and activities already included in the scope of the FATF Recommendations[14], countries should extend their regime to additional institutions, sectors or activities if they pose a higher risk of ML/TF. Countries could also consider exempting certain institutions, sectors or activities from some AML/CFT obligations where specified conditions are met, such as an assessment that the ML/TF risks associated with those sectors or activities are low[15].
- How those subject to the AML/CFT regime should be supervised for compliance with this regime: AML/CFT supervisors should consider a bank's own risk assessment and mitigation, and acknowledge the degree of discretion allowed under the national RBA, while INR 26 further requires supervisors to themselves adopt a RBA to AML/CFT supervision; and
- How those subject to the AML/CFT regime should comply: where the ML/TF risk associated with a situation is higher, competent authorities and banks have to take enhanced measures to mitigate the higher risk. This means that the range, degree, frequency or intensity of controls conducted will be stronger. Conversely, where the ML/TF risk is lower, standard AML/CFT measures may be reduced, which means that each of the required measures has to be applied, but the degree, frequency or the intensity of the controls conducted will be lighter.[16]

---

13 The effectiveness of risk-based prevention and mitigation measures will be assessed as part of the mutual evaluation of the national AML/CFT regime. The effectiveness assessment will measure the extent to which a country achieves a defined set of outcomes that are central to a robust AML/CFT system and will analyse the extent to which a country's legal and institutional framework is producing the expected results. Assessors will need to take the risks, and the flexibility allowed by the RBA, into account when determining whether there are deficiencies in a country's AML/CFT measures, and their importance - FATF(2013b).

14 See FATF (2012) Glossary, definitions of "Financial institutions" and "Designated non-financial businesses and professions".

15 INR 1, paragraph 6.

16 R. 10; INR 10, footnote 33.

D. CHALLENGES

17. Implementing a RBA can present a number of challenges:

ALLOCATING RESPONSIBILITY UNDER A RBA

18. An effective risk-based regime builds on, and reflects, a country's legal and regulatory approach, the nature, diversity and maturity of its financial sector, and its risk profile. Banks' identification and assessment of their own ML/TF risk should consider national risk assessments in line with Recommendation 1, and take account of the national legal and regulatory framework, including any areas of prescribed significant risk and any mitigation measures defined at legal or regulatory level. Where ML/TF risks are higher, banks should always apply enhanced due diligence, although national law or regulation might not prescribe exactly how these higher risks are to be mitigated (e.g., varying the degree of enhanced ongoing monitoring)[17].

19. Banks may be granted flexibility in deciding on the most effective way to address other risks, including those identified in the national risk assessment or by the banks themselves. The banks' strategy to mitigate these risks has to take into account the applicable national legal, regulatory and supervisory frameworks. When deciding the extent to which banks are able to decide how to mitigate risk, countries should consider, inter alia, their banking sector's ability to effectively identify and manage ML/TF risks as well as their supervisors' expertise and resources, which should be sufficient to adequately supervise how banks manage ML/TF risks and take measures to address any failure by banks to do so. Countries may also take into account evidence from competent authorities regarding the level of compliance in the banking sector, and the sector's approach to dealing with ML/TF risk. Countries whose financial services sectors are emerging or whose legal, regulatory and supervisory frameworks are still developing, may determine that banks are not equipped to effectively identify and manage ML/TF risk and any flexibility allowed under the risk-based approach should therefore be limited. In such cases, a more prescriptive implementation of the AML/CFT requirements may be appropriate until the sector's understanding and experience is strengthened[18].

20. Institutions should not be exempted from AML/CFT supervision even where their capacity and compliance is good. However, the RBA may allow competent authorities to focus more supervisory resource on higher risk institutions.

IDENTIFYING ML/TF RISK

21. Access to accurate, timely and objective information about ML/TF risks is a prerequisite for an effective RBA. INR 1.3 requires countries to have mechanisms to provide appropriate information on the results of the risk assessments to all relevant competent authorities, financial institutions and other interested parties. Where information is not readily available, for example where competent authorities have inadequate data to assess risks, are unable to share important information (i.e. due to its sensitivity) on ML/TF risks and threats, or where access to information is

17 R. 1.

18 This could be based on a combination of elements described in Section II, as well as objective criteria such as mutual evaluation reports, follow-up reports or FSAP.

restricted by, for example, censorship or data protection provisions, it will be difficult for banks to correctly identify (i.e., find and list) ML/TF risk and therefore may fail to assess and mitigate it appropriately.

ASSESSING ML/TF RISK

22. Assessing ML/TF risk means that countries, competent authorities and banks have to determine how the ML/TF threats identified will affect them. They should analyse the information obtained to understand the likelihood of these risks occurring, and the impact that these would have, on the individual banks, the banking sector and possibly on the national economy for large scale, systemic financial institutions, if they did occur[19]. As a result of a risk assessment, ML/TF risks are often classified as low, medium and high, with possible combinations between the different categories (medium-high; low-medium, etc.). This classification is meant to assist understanding ML/TF risks and to help prioritise them. Assessing ML/TF risk therefore goes beyond the mere collection of quantitative and qualitative information: it forms the basis for effective ML/TF risk mitigation and should be kept up-to-date to remain relevant.

23. Assessing and understanding risks means that competent authorities and banks should have skilled and trusted personnel, recruited through fit and proper tests, where appropriate. This also requires them to be technically equipped to carry out this work, which should be commensurate with the complexity of the bank's operations.

MITIGATING ML/TF RISK

24. The FATF Recommendations require that, when applying a RBA, banks, countries and competent authorities decide on the most appropriate and effective way to mitigate the ML/TF risk they have identified. This implies that they should take enhanced measures to manage and mitigate situations in which the ML/TF risk is higher; and that, correspondingly, in low risk situations, exemptions or simplified measures may be applied[20]:

- Countries looking to exempt certain institutions, sectors or activities from some of their AML/CTF obligations should assess the ML/TF risk associated with these financial institutions, activities or designated non-financial businesses and professions (DNFBPs) and be able to demonstrate that the risk is low, and that the specific conditions required for one of the exemptions of INR 1.6 are met. The complexity of the risk assessment will depend on the type of institution, sector or activity, product or services offered and the geographic scope of the activities that stands to benefit from the exemption.
- Countries and banks looking to apply simplified measures should conduct an assessment of the risks connected to the category of customers or products targeted and establish the lower level of the risks involved, and

19 Banks are not necessarily required to perform probability calculations, which may not be meaningful given the unknown volumes of illicit transactions.

20 Subject to the national legal framework providing for Simplified Due Diligence.

define the extent and the intensity of the required AML/CFT measures. Specific Recommendations set out in more detail how this general principle applies to particular requirements[21].

DEVELOPING A COMMON UNDERSTANDING OF THE RBA

25. The effectiveness of a RBA depends on a common understanding by competent authorities and banks of what the RBA entails, how it should be applied and how ML/TF risks should be addressed. In addition to a legal and regulatory framework that spells out the degree of discretion, banks have to deal with the risks they identify, and it is important that competent authorities and supervisors in particular issue guidance to banks on how they expect them to meet their legal and regulatory AML/CFT obligations in a risk-sensitive way. Supporting ongoing and effective communication between competent authorities and banks is an essential prerequisite for the successful implementation of a RBA.

26. It is important that competent authorities acknowledge that in a risk-based regime, not all banks will adopt identical AML/CFT controls and that a single isolated incident of insignificant, crystallised risk may not necessarily invalidate the integrity of a bank's AML/CFT controls. On the other hand, banks should understand that a flexible RBA does not exempt them from applying effective AML/CFT controls.

27. Countries and competent authorities should take account of the need for effective supervision of all entities covered by AML/CFT requirements. This will support a level playing field between all banking service providers and avoid that higher risk activities shift to institutions with insufficient or inadequate supervision.

FINANCIAL INCLUSION

28. Being financially excluded does not automatically equate to low or lower ML/TF risk; rather it is one factor in a holistic assessment. Financial exclusion can affect both individuals and businesses, and have many reasons. For individuals, this can include a poor credit rating or a customer's criminal background and institutions should not, therefore, apply simplified due diligence measures or exemptions solely on the basis that the customer is financially excluded.

29. A RBA may help foster financial inclusion, especially in the case of low-income individuals who experience difficulties in accessing the regulated financial system. When applying a RBA, countries may therefore establish specific cases for exemptions in the application of FATF Recommendations (based on proven low risks)[22], or allow financial institutions to be more flexible

---

21 For example, R. 10 on Customer Due Diligence.

22 As a general rule, CDD measures including the prohibition for financial institutions to keep anonymous accounts or accounts in obviously fictitious names, have to apply in all cases. Nevertheless, paragraphs 2 and 6 of INR 1 provide that: "*Countries may also, in strictly limited circumstances and where there is a proven low risk of ML/TF, decide not to apply certain Recommendations to a particular type of financial institution or activity, or DNFBP*"… and "*Countries may decide not to apply some of the FATF Recommendations requiring financial institutions or DNFBPs to take certain actions, provided: (a) there is a proven low risk of ML and TF; this occurs in strictly limited and justified circumstances; and it relates to a particular type of financial institution or activity, or DNFBP*" (para.6). This exemption has been implemented by different countries in the interest of financial inclusion policies. See also paragraphs 56

in their application of CDD measures in case of lower ML/TF risks. In this context, financial inclusion will contribute to greater transparency and traceability of financial flows.

and 57 of the FATF Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion on the main challenges for countries seeking to make use of the proven low risk exemption.

SECTION II – GUIDANCE FOR SUPERVISORS

30. The RBA to AML/CFT aims to develop prevention or mitigation measures which are commensurate to the ML/TF risks identified. In the case of supervision, this applies to the way supervisory authorities allocate their resources. It also applies to supervisors discharging their functions in a way that is conducive to the application of a risk-based approach by banks.

A. THE RISK-BASED APPROACH TO SUPERVISION

31. Recommendation 26 requires countries to subject banks to adequate AML/CFT regulation and supervision. INR 26 requires supervisors to allocate supervisory resources to areas of higher ML/TF risk, on the basis that supervisors understand the ML/TF risk in their country and have on-site and off-site access to all information relevant to determining a bank's risk profile.

Box 1. **Additional sources of information**

Report by the European Supervisory Authorities

In October 2013, the European Supervisory Authorities (European Insurance and Occupational Pensions Authority (EIOPA) for insurance and occupational pensions, European Banking Association (EBA) for banking and European Securities and Markets Authority (ESMA) for securities) published a *Preliminary report on anti-money laundering and counter financing of terrorism risk-based supervision*. This report builds on the FATF Standards and sets out what the RBA to AML/CFT supervision entails. It also lists a series of self-assessment questions supervisors may ask themselves when reviewing their approach.

BCBS Guidelines

In January 2014, the Basel Committee on Banking Supervision (BCBS) published a set of guidelines to describe how banks should include the management of risks related to money laundering and financing of terrorism within their overall risk management framework, *"Sound management of risks related to money laundering and financing of terrorism"*. These guidelines are intended to support the implementation of the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation issued by the FATF in 2012. In no way should they be interpreted as modifying the FATF standards, either by strengthening or weakening them[1]. The FATF's present Guidance provides a general framework for the application of the RBA, by supervisors and the banking sector. More detailed guidelines on the implementation of the RBA by supervisors can be found in the BCBS document.

1. BCBS (2014a), par. 3.

UNDERSTANDING ML/TF RISK

32. Supervisors should understand the ML/TF risks to which the banking sector is exposed[23], and the ML/TF risks associated with individual banks and banking groups. Supervisors should draw on a variety of sources to identify and assess ML/TF risks.

33. For sectoral risks, these are likely to include, but will not be limited to, the jurisdiction's national risk assessments, domestic or international typologies and supervisory expertise, as well as Financial Intelligence Unit (FIU) feedback.

34. For individual banks, supervisors should take into account the level of inherent risk including the nature and complexity of the bank's products and services, their size, business model, corporate governance arrangements, financial and accounting information, delivery channels, customer profiles, geographic location and countries of operation. Supervisors should also look at the controls in place, including the quality of the risk management policy, the functioning of the internal oversight functions etc.

35. Some of this information can be obtained through prudential supervision. Other information, which may be relevant in the AML/CFT context, includes the fit and properness of the management and the compliance function[24]. This involves information-sharing and collaboration between prudential and AML/CFT supervisors, especially when the responsibilities belong to two separate agencies.

36. Information from the bank's other stakeholders such as other supervisors, the FIU and law enforcement agencies may also be helpful in determining the extent to which a bank is able to effectively manage the ML/TF risk to which it is exposed.

37. Supervisors should review their assessment of both the sector's and banks' ML/TF risk profile periodically and in any case when a bank's circumstances change or relevant new threats emerge.

Examples of different ways banking supervisors assess ML/TF risk in the banking sector and in individual banks can be found in Annex 1.

MITIGATING ML/TF RISK

38. The FATF Recommendations[25] require supervisors to allocate more supervisory resources to areas of higher ML/TF risk. This means that supervisors should determine the frequency and intensity of periodic assessments based on the level of ML/TF risk to which the sector and individual banks are exposed. It also means that where detailed supervision of all banks for AML/CFT purposes is not feasible, supervisors should give priority to the areas of higher risk, either in the individual banks or to banks operating in a particular sector.

---

23 Consistent with Basel Core Principle (BCP) 8 (BCBS, 2011).

24 As specified in BCP 5.

25 In line with BCP 9.

39. Examples of ways in which supervisors can adjust their approach include:

a) Adjusting the intensity of checks required to perform their authorisation function: supervisors can adjust the level of information they require when working to prevent criminals or their associates from holding a significant or controlling interest in a bank. For example, where the ML/TF risk associated with the sector is low, the opportunities for ML/TF associated with a particular business activity may be limited and thus supervisors may decide to base their approval decisions on a review of relevant documentation. Where the ML/TF risk associated with the sector is high, supervisors may ask for additional information.

b) Adjusting the type of AML/CFT supervision: supervisors should always have both on-site and off-site access to all relevant risk and compliance information. However, to the extent permitted by their regime, supervisors can determine the correct mix of on-site and off-site supervision of banks. Off-site supervision alone may not be appropriate in higher risk situations.

c) Adjusting the frequency and nature of ongoing AML/CFT supervision: supervisors should adjust the frequency of AML/CFT supervision in line with the risks identified and combine periodic reviews and *ad hoc* AML/CFT supervision as issues emerge, e.g., as a result of whistleblowing, information from law enforcement, or other supervisory findings resulting from, for example, general prudential supervision or a bank's inclusion in thematic review samples.

Examples of different ways banking supervisors adjust the frequency of ML/TF supervision in line with the risks identified can be found in Annex 1.

d) Adjusting the intensity of AML/CFT supervision: supervisors should decide on the appropriate scope or level of assessment in line with the risks identified[26], with the aim of assessing the adequacy of banks' policies and procedures that are designed to prevent them from being abused[27]. Examples of more intensive supervision could include: detailed testing of systems and files to verify the implementation and adequacy of the bank's risk assessment, CDD, reporting and record keeping policies and processes, internal auditing, interviews with operational staff, senior management and the Board of directors and AML/CFT assessment in particular lines of business.

Examples of different ways banking supervisors adjust the intensity of ML/TF supervision in line with the risks identified can be found in Annex 1.

40. Supervisors should use their findings to review and update their ML/TF risk assessments and, where necessary, consider whether their approach to AML/CFT supervision and their AML/CFT rules and guidance remain adequate. Whenever appropriate, and in compliance with

26 BCP 11 considers early intervention to correct problems.

27 In line with BCP 29.

relevant confidentiality requirements, these findings should be communicated to banks to enable them to enhance their RBA.

41. In line with Recommendation 26 and the application of the Basel Core Principles relevant for AML/CFT[28], banking supervisors should consider the results of other prudential or financial supervision in their AML/CFT supervisory activities. Similarly, they should check that the broader prudential findings that drive the overall supervisory strategies of banks are informed by, and adequately address, the findings of the AML/CFT supervisory programme.

B. SUPERVISION OF THE RISK-BASED APPROACH

GENERAL APPROACH

42. It is important that supervisors discharge their functions in a way that is conducive to banks' adoption of a risk-based approach. This means that supervisors have to take steps to check that their staff are equipped to assess whether a bank's policies, procedures and controls are appropriate in view of the risks identified through the risk assessment, and its risk appetite[29]. Supervisors should make sure that the bank adheres to its own policies, procedures and controls, and that decisions are made using sound judgment. It also implies that supervisors articulate and communicate clearly their expectations of the measures needed for banks to comply with the applicable legal and regulatory framework. The aim is that supervisory actions are in most cases predictable, consistent and proportionate and to this end, training of supervisory staff and the effective communication of expectations to banks are key.

43. To support supervisors' understanding of the overall strength of measures in the banking sector, carrying out comparisons between banks' AML/CFT programmes could be considered as a means to inform their judgment of the quality of an individual bank's controls. Supervisors should, however, note that under the RBA, there may be valid reasons why banks' controls differ: supervisors should be equipped to evaluate the merits of these differences, especially when comparing banks with differing levels of operational complexity.

44. Supervisors should understand the ML/TF risks faced by the sector and by the banks. They should, in particular, have a thorough understanding of higher and lower risk lines of business, leading to a sound judgment about the proportionality and adequacy of AML/CFT controls. Supervisors should engage in a dialogue with individual banks about their views on AML/CFT controls set up by that institution.

45. The general principles outlined above in relation to domestic banks and domestic banking groups also apply to international banking groups. The application is, however, more complex as it involves legal frameworks and risks of more than one jurisdiction and also supervision by more

28 Basel Committee on Banking Supervision (BCBS) Principles 1-3, 5-9, 11-15, 26, and 29, see Annex 2.

29 See also Financial Stability Board (2014).

than one national supervisory body[30]. The BCBS's "*Sound management of risks related to money laundering and financing of terrorism*" contains more information.[31]

TRAINING

46. INR 26 provides that supervisory staff in charge of the supervision of banks in their implementation of a risk-based approach should understand the degree of discretion a bank has in assessing and mitigating its ML/TF risks. In particular, supervisors should check that staff have been trained to assess the quality of a bank's ML/TF risk assessments and to consider the adequacy, proportionality and effectiveness of the bank's AML/CFT policies, procedures and internal controls in light of this risk assessment.

47. Training should allow supervisory staff to form sound judgments about the adequacy and proportionality of a bank's AML/CFT controls. It should also aim at achieving consistency in the supervisory approach conducted at national level, in case of multiple competent supervisory authorities or because of the national supervisory model.

GUIDANCE

48. Supervisors should communicate their expectations of banks' compliance with their legal and regulatory obligations[32], after considering engaging in a consultative process with relevant stakeholders. This guidance may be in the form of high-level requirements based on desired outcomes, risk-based rules, information about how supervisors interpret relevant legislation or regulation, or more detailed guidance about how particular AML/CFT controls are best applied. Supervisors should also consider issuing guidance to banks on how to comply with their legal and regulatory AML/CFT obligations in a way that fosters financial inclusion.

49. Where supervisors' guidance remains high-level and principles-based, guidance written by industry sectors on how to meet the legal and regulatory obligations may be useful for explanatory and operational purposes. Banks should note, however, that the private sector guidance they take into consideration should be consistent with national legislation, based on international standards, and guidelines issued by competent authorities.

Examples of different approaches to banking supervisory guidance can be found in Annex 1.

50. Supervisors should consider liaising with other relevant domestic regulatory and supervisory authorities to secure a coherent interpretation of the legal obligations and to minimise disparities. This is particularly important where more than one supervisor is responsible for supervision (for example, where the prudential supervisor and the AML/CFT supervisors are in different agencies, or in separate divisions of the same agency). Multiple guidance should not create opportunities for regulatory arbitrage, loopholes or unnecessary confusion among banks. When possible, relevant regulatory and supervisory authorities should consider preparing joint guidance.

---

30 General supervisory standard set out in BCPs 12 and 13.

31 Part IV. See also BCBS (2010b), and BCBS (2014a) (Consultative document) on collaboration and exchanges of information between home and host supervisors.

32 R. 34.

SECTION III – GUIDANCE FOR BANKS

51. The RBA to AML/CFT aims to support the development of prevention and mitigation measures that are commensurate to the ML/TF risks identified. In the case of banks, this applies to the way banks allocate their compliance resources, organise their internal controls and internal structures, and implement policies and procedures to deter and detect ML/TF, including, where relevant, at group level.

52. Banking encompasses a wide range of financial products and services, which are associated with different ML/TF risks. These include, but are not limited to:

- *Retail banking*, where banks offer products and services directly to personal and business customers (including legal arrangements), such as current accounts, loans (including mortgages) and savings products;
- *Corporate and investment banking,* where banks provide corporate finance and corporate banking products and investment services to corporations, governments and institutions;
- *Investment services (or wealth management)*, where banks provide products and services to manage their customers' wealth (sometimes referred to as private banking); and
- *Correspondent services*, where banking services are provided by one bank (the "correspondent bank") to another bank (the "respondent bank")[33].

53. Banks should be mindful of those differences when assessing and mitigating the ML/TF risk to which they are exposed.

A. RISK ASSESSMENT

54. The risk assessment forms the basis of a bank's RBA. It should enable the bank to understand how, and to what extent, it is vulnerable to ML/TF. It will often result in a stylised categorisation of risk, which will help banks determine the level of AML/CFT resources necessary to mitigate that risk. It should always be properly documented, maintained and communicated to relevant personnel within the bank.

55. A bank's risk assessment need not be complex, but should be commensurate with the nature and size of the bank's business. For smaller or less complex banks, (for example where the bank's customers fall into similar categories and/or where the range of products and services the bank offers are very limited), a simple risk assessment might suffice. Conversely, where the bank's products and services are more complex, where there are multiple subsidiaries or branches offering a wide variety of products, and/or their customer base is more diverse, a more sophisticated risk assessment process will be required.

[33] See FATF Glossary (FATF, 2012).

56. In identifying and assessing the ML/TF risk to which they are exposed, banks should consider a range of factors which may include:

- The nature, scale, diversity and complexity of their business;
- Their target markets;
- The number of customers already identified as high risk;
- The jurisdictions the bank is exposed to, either through its own activities or the activities of customers, especially jurisdictions with relatively higher levels of corruption or organised crime, and/or deficient AML/CFT controls and listed by FATF;
- The distribution channels, including the extent to which the bank deals directly with the customer or the extent to which it relies (or is allowed to rely on) third parties to conduct CDD and the use of technology;
- The internal audit and regulatory findings;
- The volume and size of its transactions, considering the usual activity of the bank and the profile of its customers.[34]

57. Banks should complement this information with information obtained from relevant internal and external sources, such as heads of business, relationship managers, national risk assessments, lists issued by inter-governmental international organisations and national governments, AML/CFT mutual evaluation and follow-up reports by FATF or associated assessment bodies as well as typologies. They should review their assessment periodically and in any case when their circumstances change or relevant new threats emerge.

Box 2. **Examples of ML/TF risk associated with different banking activities[1]:**

- ***Retail banking:*** provision of services to cash-intensive businesses, volume of transactions, high-value transactions, diversity of services.
- ***Wealth management:*** culture of confidentiality, difficulty to identify beneficial owners, concealment (use of offshore trusts), banking secrecy, complexity of financial services and products, PEPs, high value transactions, multiple jurisdictions.
- ***Investment banking:*** layering and integration, transfer of assets between parties in exchange for cash or other assets, global nature of markets.
- ***Correspondent banking:*** high value transactions, limited information about the remitter and source of funds especially when executing transactions with a bank located in a jurisdiction that does not comply or complies insufficiently with FATF Recommendations, the possibility that PEPs are involved regarding the ownership of a bank.

1. The proposed categorisation of banking activities is purely indicative (see par. 52) and the list of identified risks is illustrative and non-exhaustive.

34 INR 1 and 10.

58. The risk assessment should be approved by senior management and form the basis for the development of policies and procedures to mitigate ML/TF risk, reflecting the risk appetite of the institution and stating the risk level deemed acceptable. It should be reviewed and updated on a regular basis. Policies, procedures, measures and controls to mitigate the ML/TF risks should be consistent with the risk assessment.

B. RISK MITIGATION

IDENTIFICATION, VERIFICATION AND THE PURPOSE AND INTENDED NATURE OF THE BUSINESS RELATIONSHIP

59. Banks should develop and implement policies and procedures to mitigate the ML/TF risks they have identified through their individual risk assessment. Customer due diligence (CDD) processes should be designed to help banks understand who their customers are by requiring them to gather information on what they do and why they require banking services. The initial stages of the CDD process should be designed to help banks assess the ML/TF risk associated with a proposed business relationship, determine the level of CDD to be applied and deter persons from establishing a business relationship to conduct illicit activity.

60. Based on a holistic view of the information obtained in the context of their application of CDD measures, banks should be able to prepare a customer risk profile. This will determine the level and type of ongoing monitoring and support the bank's decision whether to enter into, continue or terminate, the business relationship. Risk profiles can apply at the individual customer level or, where groups of customers display homogenous characteristics (for example, clients with similar income range, or conducting similar types of banking transactions) can be applied to such groups. This approach is particularly relevant for retail banking customers.

61. Initial CDD comprises:

- Identifying the customer and, where applicable, the customer's beneficial owner;
- Verifying the customer's identity on the basis of reliable and independent information, data or documentation to at least the extent required by the applicable legal and regulatory framework; and
- Understanding the purpose and intended nature of the business relationship and, in higher risk situations, obtaining further information.

62. In addition, banks should take measures to comply with national and international sanctions legislation by screening the customer's and beneficial owner's names against the UN and other relevant sanctions lists.

63. As a general rule, CDD measures have to apply in all cases. The extent of these measures may be adjusted, to the extent permitted or required by regulatory requirements, in line with the ML/TF risk, if any, associated with the individual business relationship as discussed above under *Risk Assessment*. This means that the amount and type of information obtained, and the extent to which this information is verified, must be increased where the risk associated with the business relationship is higher. It may also be simplified where the risk associated with the business

relationship is lower. Banks therefore have to draw up, and periodically update, customer risk profiles[35], which serve to help banks apply the appropriate level of CDD.

Box 3. **Examples of Enhanced Due Diligence/Simplified Due Diligence measures (see also INR 10)**

- Enhanced Due Diligence (EDD)
  - obtaining additional identifying information from a wider variety or more robust sources and using the information to inform the individual customer risk assessment
  - carrying out additional searches (e.g., verifiable adverse media searches) to inform the individual customer risk assessment
  - commissioning an intelligence report on the customer or beneficial owner to understand better the risk that the customer or beneficial owner may be involved in criminal activity
  - verifying the source of funds or wealth involved in the business relationship to be satisfied that they do not constitute the proceeds from crime
  - seeking additional information from the customer about the purpose and intended nature of the business relationship
- Simplified Due Diligence (SDD)
  - obtaining less information (e.g., not requiring information on the address or the occupation of the potential client), and/or seeking less robust verification, of the customer's identity and the purpose and intended nature of the business relationship
  - postponing the verification of the customer's identity

Box 4. **CDD and financial inclusion considerations**

The application of a RBA to CDD may support financial inclusion objectives by providing for a more flexible application of CDD measures to certain categories of financial products or customers who might otherwise struggle to meet banks' CDD requirements. However, financial exclusion in itself is not an indicator of low ML/TF risk and banks have to take an informed decision, based on a holistic assessment of ML/TF risk, whether exemptions or SDD measures may be appropriate.

64. Where banks cannot apply the appropriate level of CDD, Recommendation 10 requires that banks do not enter into the business relationship or terminate the business relationship.

65. The BCBS's guidance on the *Sound management of risk related to money laundering and financing of terrorism* provides detailed guidance to banks on the management of money laundering

35 based on the bank's own risk assessment and taking into account risk factors such as those outlined in the FATF standards, e.g., in INR 10 and Recommendations/INR 12-16.

risk in correspondent banking and in situations where banks rely on third parties to carry out all, or part, of their initial CDD.

ONGOING CDD/MONITORING

66. Ongoing monitoring means the scrutiny of transactions to determine whether those transactions are consistent with the bank's knowledge of the customer and the nature and purpose of the banking product and the business relationship. Monitoring also involves identifying changes to the customer profile (for example, their behaviour, use of products and the amount of money involved), and keeping it up to date, which may require the application of new, or additional, CDD measures. Monitoring transactions is an essential component in identifying transactions that are potentially suspicious.

67. Monitoring should be carried out on a continuous basis or triggered by specific transactions. It could also be used to compare a customer's activity with that of a peer group. It need not require electronic systems, although for some types of banking activity, where large volumes of transactions occur on a regular basis, automated systems may be the only realistic method of monitoring transactions. However, where automated systems are used, banks should understand their operating rules, verify their integrity on a regular basis and check that they address the identified ML/TF risks.

68. Banks should adjust the extent and depth of monitoring in line with their institutional risk assessment and individual customer risk profiles. Enhanced monitoring should be required for higher risk situations, while banks may decide to reduce the frequency and intensity of monitoring where the risks are lower. The adequacy of monitoring systems and the factors leading banks to adjust the level of monitoring should be reviewed regularly for continued relevance to the bank's AML/CFT risk programme.

69. Banks should document and state clearly the criteria and parameters used for customer segmentation and for the allocation of a risk level for each of the clusters of customers. Criteria applied to decide the frequency and intensity of the monitoring of different customer segments should also be transparent.

Box 5. **Examples of monitoring in high/lower risk situations**

- Monitoring in high risk situations: daily transaction monitoring, manual transaction monitoring, frequent analysis of information, considering the destination of funds, establishment of red flags based on typologies reports, reporting of monitoring results to senior management etc.
- Monitoring in lower risk situations: thresholds, low frequency, automated systems

The BCBS's guidance on the *Sound management of risk related to money laundering and financing of terrorism* sets out in Section II 1 (d) what banks should consider when assessing whether their monitoring system is adequate. It stresses that a bank should have a monitoring system in place that is adequate with respect to its size, its activities and complexity as well as the risks present in the bank. For most banks, especially those which are internationally active, effective monitoring is likely to necessitate the automation of the monitoring process.

70. To this end, banks should properly document, retain and communicate to the relevant personnel the results of their monitoring as well as any queries raised and resolved.

REPORTING

71. Recommendation 20 requires countries to mandate that if a bank suspects, or has reasonable grounds to suspect, that funds are the proceeds of crime or are related to terrorist financing, it shall report its suspicions promptly to the relevant FIU. Banks should have the ability to flag unusual movement of funds or transactions for further analysis. Banks should have appropriate case management systems so that such funds or transactions are scrutinised in a timely manner and a determination made as to whether the funds or transaction are suspicious.

72. Funds or transactions that are suspicious should be reported promptly to the FIU and in the manner specified by competent authorities. The processes banks put in place to escalate suspicions and, ultimately, report to the FIU, should reflect this. While the policies and processes leading banks to form a suspicion can be applied on a risk-sensitive basis, a bank should report once ML/TF suspicion has formed.

C. INTERNAL CONTROLS, GOVERNANCE AND MONITORING

INTERNAL CONTROLS

73. Adequate internal controls are a prerequisite for the effective implementation of policies and processes to mitigate ML/TF risk. Internal controls include appropriate governance arrangements where responsibility for AML/CFT is clearly allocated, controls to monitor the integrity of staff, in accordance with the applicable local legislation, especially in cross-border situations and the national risk assessment, compliance and controls to test the overall effectiveness of the bank's policies and processes to identify, assess and monitor risk.

74. For larger banking groups, there should be controls in place for a consistent approach to AML/CFT controls across the group. The BCBS's *"Sound management of risk related to money laundering and financing of terrorism"* document[36] provides comprehensive guidance to banks on the effective management of ML/TF risk in a group-wide and cross-border context[37].

---

36 See part III.

37 It explains the rationale behind and principles of consolidated risk management; how group-wide AML/CFT policies and procedures should be consistently applied and supervised across the group, and, where reflecting local business considerations and the requirements of the host jurisdiction, should still be consistent with and supportive of the broader policies and procedures of the group; how banks should address differences in home/host requirements. Importantly, it also provides detail on how banks that are part of a group should share information with members of the same group with a view to informing and strengthening group-wide risk assessment and the implementation of effective group-wide AML/CFT policies and procedures.

GOVERNANCE

75. The successful implementation and effective operation of a RBA to AML/CFT depends on strong senior management leadership and oversight of the development and implementation of the RBA across the bank.

76. Senior management should consider various ways to support AML/CFT initiatives:

- promote compliance as a core value of the bank by sending a clear message that the bank will not enter into, or maintain, business relationships that are associated with excessive ML/TF risks which cannot be mitigated effectively. Senior management, together with the board, are responsible for setting up robust risk management and controls adapted to the bank's stated, sound risk-taking policy;
- implement adequate mechanisms of internal communication related to the actual or potential ML/TF risks faced by the bank. These mechanisms should link the board of directors, the AML/CFT chief officer, any relevant or specialised committee within the bank (e.g., the risks or the ethics/compliance committee)[38], the IT division and each of the business areas;
- decide on the measures needed to mitigate the ML/TF risks identified and on the extent of residual risk the bank is prepared to accept; and
- adequately resource the bank's AML/CFT unit.

Box 6. **Examples of steps taken by banks' senior management to promote compliance:**

- To carry out product development and commercial campaigns in strict compliance with national AML/CFT legislation.
- To involve senior management in AML/CFT training of staff.

77. This implies that senior management should not only know about the ML/TF risks to which the bank is exposed but also understand how its AML/CFT control framework operates to mitigate those risks. This would require that senior management:

- receives sufficient, regular and objective information to get an accurate picture of the ML/TF risk to which the bank is exposed through its activities and individual business relationships;
- receives sufficient and objective information to understand whether the bank's AML/CFT controls are effective (for example information from the Chief Compliance Officer on the effectiveness of control, or audit reports);

38 BCBS(2010a), par. 52 and 53.

- and that processes are in place to escalate important decisions that directly impact the ability of the bank to address and control risks.

78. It is important that responsibility for the consistency and effectiveness of AML/CFT controls be clearly allocated to an individual of sufficient seniority within the bank to signal the importance of ML/TF risk management and compliance, and that ML/TF issues are brought to senior management's attention. This includes, but is not restricted to, the appointment of a skilled compliance officer at management level[39].

ENSURING AND MONITORING COMPLIANCE

79. A bank's internal control environment should be conducive to assuring the integrity, competence and compliance of staff with relevant policies and procedures. The measures relevant to AML/CFT controls should be consistent with the broader set of controls in place to address business, financial and operating risks generally.

VETTING, RECRUITMENT AND REMUNERATION

80. Banks should check that staff they employ have integrity and are adequately skilled and possess the knowledge and expertise necessary to carry out their function, in particular where staff are responsible for implementing AML/CFT controls.

81. The level of vetting procedures of staff should reflect the ML/TF risks to which individual staff are exposed and not focus merely on senior management roles. Steps should be taken to manage potential conflicts of interest for staff with AML/CFT responsibilities. Their remuneration should be in line with principles on the independence of the compliance function in the BCBS paper on principles on compliance and the compliance function in banks[40].

TRAINING AND AWARENESS

82. The effective application of AML/CFT policies and procedures depends on staff within banks understanding not only the processes they are required to follow but also the risks these processes are designed to mitigate, as well as the possible consequences of those risks. It is therefore important that bank staff receive AML/CFT training, which should be:

- Of high quality, relevant to the bank's ML/TF risks, business activities and up to date with the latest legal and regulatory obligations, and internal controls;
- Obligatory for all relevant staff;
- Tailored to particular lines of business within the bank, equipping staff with a sound understanding of specialised ML/TF risks they are likely to face and their obligations in relation to those risks;

39 INR 18.

40 BCBS (2005).

- Effective: training should have the desired effect, and this can be checked for example by requiring staff to pass tests or by monitoring levels of compliance with the bank's AML/CFT controls and applying appropriate measures where staff are unable to demonstrate the level of knowledge expected;
- Ongoing: in line with INR 18, AML/CFT training should be regular, relevant, and not be a one-off exercise when staff are hired;
- Complemented by AML/CFT information and updates that are disseminated to relevant staff as appropriate.

83. Overall, the training should also seek to build up a working behaviour where compliance is embedded in the activities and decisions of all bank's staff.

ASSESSMENT OF CONTROLS

84. Banks should take steps to be satisfied that their AML/CFT policies and controls are adhered to and effective. To this end, their controls should be monitored on an ongoing basis by the bank's compliance officer. In addition, the adequacy of and compliance with banks' AML/CFT controls should be reviewed by an audit function.

85. Recommendation 18 requires countries to require banks to appoint a compliance officer at management level. In addition to advising relevant staff how to meet their obligations, their role should be to monitor and assess ML/TF risks across the bank as well as the adequacy and effectiveness of the measures the bank has put in place to mitigate the risks. The compliance officer should therefore have the necessary independence, authority, seniority, resources and expertise to carry out these functions effectively, including the ability to access all relevant internal information (including across lines of business, and foreign branches and subsidiaries).

Box 7. **Examples of internal controls to encourage compliance**

- Facilitate the reporting of suspicious transactions:
  - Set up staff training on mechanisms to adequately detect unusual transactions
  - Establish adequate channels to allow staff to report unusual transactions to the Compliance Officer
  - Ensure confidentiality to staff reporting suspicious transactions
- Allow staff to report areas of policy or controls they find unclear/unhelpful/ineffective:
  - Establish ongoing consultation channels for staff concerning AML/CFT issues
  - Ensure consistency of the answers given to staff questions concerning AML/CFT issues
  - Conduct AML/CFT activities in such a way that they are perceived by all staff as a support to the quality of the banking services provided to clients and the integrity of the bank.

86. Recommendation 18 also requires countries to require banks to have an independent audit function to test the bank's AML/CFT programme with a view to establishing the effectiveness of the bank's overall AML/CFT policies and processes and the quality of its risk management across its operations, departments, branches and subsidiaries, both domestically and, where relevant, abroad. The findings should inform senior management's view of the design and implementation of the bank's AML/CFT framework. The audit function needs to examine the adequacy of all risk determinations and should therefore not focus exclusively on higher risks.

87. Both the compliance and audit functions should base their assessment on all information relevant to their task including, where relevant and appropriate, information obtained confidentially through relevant internal mechanisms or whistleblowing hotlines. Other sources of information can include training pass rates, compliance failures, and analysis of questions received from staff.

ANNEX 1

EXAMPLES OF COUNTRIES' SUPERVISORY PRACTICES FOR THE IMPLEMENTATION OF THE RISK-BASED APPROACH TO THE BANKING SECTOR

This annex shares countries' supervisory practices which seek to illustrate the implementation of the RBA. They are presented as examples only. At the time of the publication of this guidance, the individual efforts had not been assessed for compliance with FATF Recommendations as part of the 4th Round of mutual evaluations. Therefore, their presentation here should not be considered as an endorsement by FATF.

Examples of different ways banking supervisors assess ML/TF risks in the banking sector and in individual banks

AUSTRALIA

Australia's AML/CFT regulator and specialist financial intelligence unit, AUSTRAC, applies a risk-based approach to the supervision of the banking sector at a corporate group level. Under this approach, AUSTRAC applies higher amounts of regulatory effort towards supervising entities within corporate groups that provide services and products identified as having a higher exposure and vulnerability to ML/TF risk.

Four factors are taken into account in determining the ML/TF risk profile:

- Whether the reporting entity group (RE Group) operates within an industry type identified as a major or significant channel for money laundering (as set out in Australia's National Threat Assessment on money laundering). RE Groups within these industry types are subject to higher levels of supervision by AUSTRAC.
- The exposure of an RE Group to ML/TF risk. Proxy measures used by AUSTRAC to determine the exposure of an RE Group to ML/TF activities are the size of the entity and/or the volume and value of transaction reports lodged with AUSTRAC. Larger RE Groups generally have more customers and typically provide products which are more complex using multiple distribution channels in multiple jurisdictions. In addition, large RE Groups have a greater impact on the overall integrity of Australia's financial system. Accordingly, large RE Groups, particularly those that lodge significant numbers of transaction reports with AUSTRAC, are subject to higher levels of supervision.

- Specific interest by AUSTRAC's Intelligence operations in relation to particular RE Groups or industry sectors.
- Specific interest by competent authorities (law enforcement, intelligence, revenue or regulatory agencies) in relation to particular RE Groups.

GERMANY

BaFin's risk classification of financial institutions is a combination of:

- The assessment of an individual abstract risk situation, based on 5 essential risk criteria (location, scope of business, product structure, customer structure and distribution structure). Each of the 5 elements is rated. The rating reached on customer structure weights more in the overall rating, as ML is a crime committed by customers. If the financial institution reaches an overall score which is the high limit for low risk institutions, or the low limit for enhanced risk institutions, the supervisor has discretion to decide which risk category the institution will fall in, based on its past AML/CFT history.
- The assessment of the quality of AML/CFT preventive measures (task fulfilment by the AML compliance officer, IT monitoring, Know-Your-Customer measures etc.) implemented by the financial institution, including the group-wide compliance aspects when relevant. The ratings are based on information from the annual audit reports and additional assessments from external auditors. The importance and scope of the deficiencies identified will impact the quality level and the rating of preventive measures.

The end result is a 12 cell-matrix, which will be used to determine the intensity of the AML/CFT supervision required:

		Quality of AML/CFT-prevention			
		A (high)	B (medium-high)	C (medium-low)	D (low)
Potential threat of ML/TF	3 (high)	3A	3B	3C	3D
	2 (medium)	2A	2B	2C	2D
	1 (low)	1A	1B	1C	1D

MEXICO

The National Banking and Securities Commission (CNBV), based on the inherent risks identified through the information obtained from financial institutions and other sources, establishes monitoring strategies. The strategy for effective monitoring takes into account which products or services are offered by financial entities, their types of users or customers, their flow of funds, and their geographic area of operation, among others. Considering those factors, CNBV determines which financial institutions represent higher risks in order to decide which financial institutions have to be visited during the year (annual program). Subsequently, a diagnosis for each entity to be visited is performed, where the major significant activities (products with inherent risk) and the correspondent risk mitigating action that the financial institutions have applied are reviewed. As a result of the inspection visit, a risk rating of the entity is determined, which at the same time provides the input necessary to determine the periodicity for further inspection visits on AML/CFT

THE NETHERLANDS

The Dutch Central Bank (DNB) is responsible for AML/CFT supervision and enforcement over banks. DNB applies a risk-based approach to AML/CFT supervision by focusing on institutions which pose the highest risk. For this, a thorough understanding of the risks is required. DNB analyses integrity risks on different levels, namely on a macro, meso and micro level. On a macro-level DNB takes into account country and global developments which are of importance for the Dutch financial sector. On a meso-level, DNB distinguishes between different sectors and the way in which different developments/risks might impact these sectors. On a micro-level DNB takes into account factors of specific institutions which can increase the vulnerability of those institutions.

The first step in the risk-based approach is to identify ML/TF risks through several sources, such as typologies, intelligence, international and national committees and other (foreign) supervisors which are involved in the prevention of ML/TF (i.e. FATF, BCBS, European Supervisory Authorities, IAIS). DNB also takes into account information received from the supervisory visits. DNB sends out a questionnaire to a group of selected institutions to gain insight in the inherent risk level and control measures in place. In addition, DNB has set up a trend analysis function which monitors open sources of information to detect new trends and signals which concern AML/CFT supervision.

When the risks are identified, DNB analyses these risks based on different criteria such as the potential impact on society, the institutions, and the stability of the financial sector. The risk profile of an institution is determined on the basis of two main dimensions, the ML/TF risk level and control level. Factors for the inherent risk score which DNB takes into account are geographical scope, the customer base of the institution, the products and services and the distribution channel of the institution. For the control level DNB look into the governance and control procedures of an institution, the adequacy of the compliance function, the compliance history and incidents and the quality of preventative measures in the institution.

SINGAPORE

The Monetary Authority of Singapore (MAS) adopts a risk-based approach in its supervision of Financial Institutions (FIs). This approach is articulated in the public monograph on MAS' *Framework for Impact and Risk Assessment of Financial Institutions*. At the heart of this framework is the impact and risk model which is used to assess FIs on two aspects annually:

- Impact (relative systemic importance): the impact assessment considers the potential impact that an FI may have on Singapore's financial system, broader economy and reputation, in the event of distress. Related institutions are grouped together for an assessment of their aggregate impact. Generally, the larger the FI's intermediary role in critical financial markets or the economy, or the greater its reach to retail customers, the higher its assessed impact.
- Risk (relative risk profile): the risk assessment examines the inherent risks of the FI's business activities, including ML/TF and proliferation financing risks, its ability to manage and control these risks, the effectiveness of its oversight and governance structure, and the adequacy of its financial resources to absorb losses and remain solvent. The assessment also takes into consideration intra-group linkages, where applicable, between the FI and its related entities, and risks posed by other entities in the group (e.g., for a locally-incorporated banking group, risks posed by significant subsidiaries will be aggregated with the main banking entity and monitored on a consolidated basis). To ensure robustness and consistency, the risk assessments of individual FIs are subjected to a process of peer comparison, challenge and review by other experienced supervisors, or panels of senior and specialist staff for key FIs.

Based on the combined assessments of impact and risk (with the impact component accorded greater weightage), the FI is assigned to one of four categories of supervisory significance, with Bucket 1 FIs supervised most intensely. FIs in Buckets 1 and 2 are supervised more closely with more resources allocated by MAS, subjected to more frequent inspections, and have their risk assessments approved by a more senior level of management.

MAS' risk-based approach encompasses both on-site and off-site supervision. MAS' off-site supervision involves ongoing monitoring of an FI's financial soundness and risk indicators, and developments in its businesses and home country, as well as trends in the financial sector. MAS also reviews the FI's regulatory returns and audit reports, and conducts regular meetings with the FI's management, auditors and home supervisors. Concerns impacting the FI's safety and soundness are followed up expeditiously.

SOUTH AFRICA

Bank Supervision Department of SARB Supervisory processes - Risk-based approach to on-site inspections

Due to limited resources, it is not practically possible to extend the scope of AML/CFT inspections to cover all areas within a bank, nor will it be possible to inspect all banks within a calendar year. Therefore, the AML Review Team, in executing its supervisory duties, has adopted a risk-based approach in scheduling and conducting AML/CFT inspections of the accountable institutions (banks) it supervises.

Risk-based methodology:

- The AML Review team will always request the bank's own AML risk assessment for purposes of inspection and review;
- As one of the contributing elements of the review of the risk assessment of a bank, a list of products and services offered by the bank, aligned with each business unit, should be requested;
- The AML Review team should assess the bank's ML risk assessment process to determine whether the bank has adequately identified the level of risk it has assumed;
- In the absence of an ML risk assessment of a particular bank, the AML Review team should perform its own risk assessment based on the structure provided by the bank and the inherent risk factors of the bank's activities;
- Should the bank's risk assessment be inadequate, the AML Review Team should complete its own risk assessment as stated above;
- The test for adequacy of the bank's risk assessment or completion of the team's own risk assessment on the bank should specifically be done for a particular inspection.
- The factors used for compiling the risk assessment should be benchmarked against the FATF Recommendations, the Basel Core Principles for Effective Banking Supervision, as well as known money laundering and terrorist financing typologies from reputable authorities.
- The banking institutions' activities, products, geographic locations and client types should be segmented between high, medium and low risk.
- Based on the risk assessment (high, medium and low risk), the AML Review Team should, thereafter, develop the scope of the inspection taking into account the identified high risk AML activities from the risk assessment.
- FATF requires countries to take appropriate steps to identify and assess money laundering and terrorist risks for the entire country on an on-going basis and in order to:
- inform potential changes to the country's AML/CFT regime, including changes to laws, regulations and measures;
- assist in allocation and prioritisation of AML/CFT resources by competent authorities; and
- make information available for ML/TF risk assessments conducted by banks.

UNITED KINGDOM

The Financial Conduct Authority (FCA) classifies all firms according to the risk they pose to the FCA's operational and statutory objectives. It also classifies all firms that are subject to the UK's AML legislation according to their money laundering risk. This is because money laundering risk does not necessarily correlate to the size of a firm. As a result, a firm in a lower conduct risk category may receive relatively more supervisory attention from an AML/CFT perspective.

When classifying firms according to money laundering risk, the FCA considers a number of factors. These include the nature of the firm's business, the products and services it offers and the jurisdictions where it is located or operates.

This risk assessment and the criteria the FCA uses to inform it, are reviewed on a regular basis and firms can be reclassified without delay as appropriate.

UNITED STATES

The Federal Banking Agencies (FBAs) supervisory processes assess whether depository institutions have established the appropriate policies, procedures, and processes based on their BSA/AML risk to identify and report suspicious activity and that they provide sufficient detail in reports to law enforcement agencies to make the reports useful for investigating suspicious transactions that are reported. To ensure consistency in the application of the BSA/AML requirements, the FBAs follow the examination procedures contained in the Federal Financial Institutions Examination Council (FFIEC)'s *Bank Secrecy Act/Anti-Money Laundering Examination Manual*. In order to effectively apply resources and ensure compliance with BSA requirements, the Manual is structured to allow examiners to tailor the BSA/AML examination scope and procedures to the specific risk profile of the depository institution. It also provides the private sector with a clear "road map" of FBA supervisory expectations and definition of the procedures that examiners will apply in evaluating compliance program effectiveness. The FBAs communicate their expectations to the private sector informally through on-going dialog with boards of directors and senior management and formally through the FFIEC BSA/AML Exam Manual, guidance and general outreach in workshops and seminars for banks based on size, location, product type and other factors and through speaking engagements sponsored by trade and industry associations. The FFIEC BSA/AML Exam Manual contains sections on identified risks associated with products and services and persons and entities that incorporate law enforcement information from reports such as the U.S. National Money Laundering Strategy and the U.S. Money Laundering Threat Assessment; on-going dialog with law enforcement representatives at the national, state and local levels and risks identified by FBA examiners based on information provided by law enforcement. This information is also used to prepare and issue guidance detailing supervisory expectations for risk management related to vulnerabilities identified in the jurisdiction and scope and plan exams.

Examples of different ways banking supervisors approach on-site and off-site ML/TF supervision in line with the risks identified

AUSTRALIA

AUSTRAC's current phase of supervision includes targeting high-risk entities for supervisory activity, and to test the effectiveness of entities' systems and controls in practice. AUSTRAC has developed data-mining techniques that scan the entire regulated entity population and bring to the surface issues and vulnerabilities that may impede reporting entities' effectiveness. Through these techniques, AUSTRAC is able to identify individual reporting entities whose behavioural characteristics are outliers to that of their peers. AUSTRAC utilises this information to identify entities requiring further supervisory engagement, particularly in lower risk sectors.

After AUSTRAC identifies ML/TF risk and significance, it determines the level and type of engagement required with an RE Group based on an assessment of its compliance risk. (Compliance risk is defined as the risk that an RE Group is non-compliant with its legislative obligations, and is a different measure to the ML/TF risk of an entity. An entity may have a high ML/TF risk but have a strong approach to its regulatory obligations, meaning that its compliance risk score will be low.)

AUSTRAC uses a range of compliance techniques to assess the adequacy of RE Groups' policies, practices, systems and controls to meet the requirements of the AML/CTF Act, including:

- Low intensity or 'engagement' activities such as enrolment processes, mail-outs, e-newsletters, forums, workshops and the development and distribution of guidance materials.
- Moderate intensity or 'heightened' activities such as processes associated with the registration of remitters, behavioural assessments, desk reviews, themed reviews and transaction monitoring directed at specific behaviours of cohorts of reporting entities.
- High intensity or 'escalated' activities such as on-site assessments and a dedicated management approach. AUSTRAC tailors these activities to individual reporting entities. They are designed to have a direct impact on improving compliance outcomes.

GERMANY

On-site inspections contain both:

- Regular annual inspections, carried-out on-site by external auditors, and
- Special/targeted inspections, on a regular basis or with respect to specific circumstances by external auditors (on behalf of the supervisor) or by the supervisor itself.

Employees of the supervisory authority accompany the external auditors in all special/targeted inspections and in some regular annual inspections.

According to the Banking Act, the supervisory authority is able to decree thematic priorities in the course of regular on-site inspections. This is done for example to check the implementation of new provisions in the AML law or when a certain type of deficiency is detected in a multitude of annual reports of different financial institutions.

Off-site supervision:

- The annual report contains an annex where the main results are highlighted in one or two brief sentences, in connection with a mark. Depending on the individual risk classification of a financial institution, in certain cases of low risk only a "quick check" of this annex is done and the whole annual report is only evaluated ("intensive check") in case of bad marks in this annex.
- After the evaluation of reports from on-site inspections and depending on their findings, the follow-up procedure will be conducted with different level of intensity.
- Detailed written information about AML measures applied to specific customer/product groups can be requested, or a consultation with the bank's compliance officer can be organised.
- The presentation of updated internal safeguards which have been put in place can be requested; depending on the importance of the system and the shortcomings that were analysed, an external expert can be mandated to check the proper operability of the system in place.

MEXICO

The AML/CFT supervision in Mexico is composed of the following stages:

- Financial institutions are assigned a risk rating using a RBA model. Information is requested periodically from financial institutions to elaborate a regulatory report and the offsite analysis is performed on the basis of this data. The information collected is consolidated in the same risk matrix used to determine the risk level of the entity. Based on these results, the CNBV determines the frequency with which a financial institution will be visited in order to supervise its compliance with AML/CFT laws and regulations; including the implementation of measures to mitigate AML/CFT risks.
- Based on the risk rating of a given financial institution, a monitoring strategy for onsite supervision is determined focusing on the higher risk factors identified at the previous stage. This is strengthened with a diagnosis that allows pinpointing significant activities (products and services) set as higher risks and the effectiveness of specific mitigants implemented by the financial institution for such activities.

- During the on-site inspections, supervisors request information and documentation in order to confirm if the risk level previously assigned to the financial institution is adequate, and conduct their inspection accordingly. Supervisors enhance their review of those aspects considered of higher risk.
- In accordance with the results of the inspections, various acts of authority can be carried out, including the issuance of observations and recommendations, as well as the implementation of corrective actions and/or sanctions.

Finally, the results of the inspection are taken into account to either confirm a risk level or assign a new one to the supervised entity. This new information is added to the offsite supervisory matrix, which helps determine the best timing for having the entity monitored again (supervision strategy).

HONG KONG, CHINA

The Hong Kong Monetary Authority (HKMA) supervises banks' AML/CFT systems through a combination of on-site examinations and off-site reviews, which is integrated as part of the broader banking supervisory process. AML/CFT supervision is risk-based, and the frequency, intensity and scope of supervisory activities are linked to the ML/TF risk profile of individual banks, which takes into account both impact to the financial system and risk level. On-site examinations comprise risk-focused examinations and thematic examinations, which are part of a cycle, culminating in best practices being provided to banks in training forums, which are conducted on an annual basis.

To illustrate the approach in practice, in 2012, the HKMA conducted thematic reviews for 9 banks over suspicious transaction reporting (STR). As a result of observations made, in Q1 and Q2 2013 a further 107 banks were subject to high-level desk-based reviews over STRs, with a focus on post-reporting risk-mitigation. On the basis of the risks identified, 26 banks were further selected for more intensive desk-based reviews, including policies and procedures and actions taken to mitigate ML/TF risks. Follow-up supervisory actions were determined on the basis of risk, including requiring additional action on the part of banks, external auditor reviews and a further 4 thematic on-site examinations that comprised interviews with key operational staff and reviews of STR related processes. The findings from this supervisory initiative were communicated to banks in training seminars held in October 2012 and April 2013, and were the subject of a guidance paper, developed in collaboration with the Joint Financial Intelligence Unit, issued on 16 December 2013.

ITALY

The Bank of Italy employs a mix of off-site and on-site supervision. Off-site analysis is systematic, carried out at set intervals, and based on analysis of data and information that banks report to the Bank of Italy (BI) (annual report of AML compliance function; reports by control bodies on specific irregularities, post inspection follow-up reports, etc.). Moreover, whenever necessary, BI holds meetings dedicated to AML issues with board members or AML compliance officers to gather relevant information and discuss initiatives.

Based on the off-site analysis results, inspections are planned and carried out. Inspections may be: full scope, targeted (business areas, specific risks, operational profiles, corrective action follow-up) and thematic. Following the entry into force of the Italian AML Law in 2008, Bank of Italy's reviewed its on-site control procedures: AML controls may be conducted in the framework of general on-site inspections or through thematic inspections dedicated to AML compliance.

In 2008, the Bank of Italy inaugurated yearly cycles of targeted on-site AML inspections on banks' branches in high risk areas in order to conduct an assessment on the implementation of AML rules in day-to-day operations. The assessment consists of short on-site visits (3/5 days) in a number of pre-selected branches located in areas of the country where specific criminal activities risks (organised crime, tax evasion, tobacco smuggling, usury, etc.) exist. Visits are conducted using a questionnaire on AML obligations (CDD, registration, reporting and training) to verify compliance with AML Law/regulations and banks' internal regulations by branch's staff; a sample testing of individual customer positions is also performed. Whenever the findings of the visits indicate major deficiencies, corrective actions are requested.

Moreover, the Italian FIU verifies compliance of financial institutions, both off-site and on-site, with regard to suspicious transactions reporting duties and cases of omitted reporting of STRs mainly on a RBA basis. The areas of risk are recognised by information transmitted by law enforcement, financial sector supervisory authorities, professional associations or other FIUs. In case of infringements or major organisational disorder at the financial institution, close coordination with Bank of Italy and other supervisory authorities is ensured by MoUs. Feedback to intermediaries, for corrective actions, is also warranted in cases detection and valuation of STRs result critical.

FRANCE

The French financial supervisor (*Autorité de Contrôle Prudentiel et de Résolution*, ACPR) implements a multi-level approach for the assessment of ML-FT risks, and the AML/CFT supervision of the financial sector:

- *Annual questionnaire on AML-CFT*: the answers to the questionnaire are systematically studied by off-site control services. Several priority levels are defined. The nature and time limit to set out corrective actions depend on the seriousness of the deficiencies revealed by the answers to the questionnaire.

  The questionnaire for credit institutions, investment firms, and life insurance institutions reflects the revised FATF Recommendations, and highlights key issues such as the RBA. It also takes account of the results of the analysis of thematic AML-CFT inspections (e.g., wealth management recently). Specific questions are added for financial groups, as well as targeted sectoral questions for the banking and insurance sectors respectively.

- *Different tools are used for the off-site control:*
  - Internal audit reports
  - On-site inspection reports

- Information collected during meetings (annual meetings, and other relevant meetings)
- Annual internal control reports, with an overview of business conducted and risks incurred by the institution; significant changes made in the internal control system; governance; money laundering and terrorist financing risks.

THE NETHERLANDS

DNB performs both on-site and off-site supervision in a risk based manner. In addition to the ongoing supervisory cycles, DNB performs thematic reviews which are in-depth reviews of a specific risk(area) for a selection of institutions. Thematic reviews allow DNB to benchmark practices, identify outliers and best practices. The process of thematic supervision starts with the selection of themes based on risk analyses, reviews from previous years or incidents/compliance issues that are known from ongoing supervision.

The entities to be visited are selected on the basis of a number of criteria, such as the size of the business, the risk profile, previous experience of compliance weaknesses etc. Prior to onsite visits, information is requested from institutions that are reviewed (such as policy and processes, transactions, suspicious transaction reports, customer information etc.). During the on-site, discussions with management, sampling of customer or transaction files as appropriate and an examination of the institution's risk assessment and risk management procedures are performed and analysed.

UNITED KINGDOM

The Financial Conduct Authority (FCA) allocates specialist supervisory resource according to the level of money laundering risk associated with a firm and *ad hoc*, as risk dictates. This involves both on-site and off-site assessments of the adequacy of firms' AML/CFT systems and controls.

Off-site assessments include the analysis of regulatory returns (which include specific financial crime questions), policies and procedures, audit reports, minutes of meetings, reports of previous supervisory visits and, where relevant, intelligence obtained through external sources.

On-site visits include interviews with key staff, testing the firm's AML/CFT controls and file reviews.

The focus and detail of both on-site and off-site reviews is determined by the reason for the review, e.g., a planned review as part of the FCA's ongoing supervisory programme or suggestions that a risk has crystallised.

Examples of differing frequency of ML/TF supervision in line with the risks identified

AUSTRALIA

The frequency of supervision by AUSTRAC correlates with the compliance risk associated with the RE Group. A key supervisory performance indicator for AUSTRAC is to undertake an assessment of

each high-risk RE Group within a three year period. In parallel, AUSTRAC employs data-mining techniques that scan the entire regulated entity population and bring to the surface issues and vulnerabilities that may impede reporting entities' effectiveness. Through these techniques, AUSTRAC is able to identify individual reporting entities whose behavioural characteristics are outliers to that of their peers. AUSTRAC utilises this information to identify entities requiring further supervisory engagement, particularly in lower-risk sectors.

GERMANY

Frequency aspects for on-site inspection are inter alia:

- Credit institutions with a total balance sheet below a specific threshold only need to be assessed on a biennial basis, except if certain risk factors indicate a higher risk.
- Special inspections are conducted more frequently with regard to "big players" in the financial market, due to the complexity of their business which requires a more frequent update of information for the supervisor.
- Special inspections can be conducted on a regular basis because of the (high) risk classification of a financial institution, regardless of its size.
- Additional or focused special inspections are sometimes conducted if serious deficiencies are evidenced by previous reports
- Special inspections can be conducted on an *ad hoc* basis in case of ML/TF related "bad news" revealed through investigations of law enforcement agencies, newspapers, whistleblowers, internet research etc.

MEXICO

The AML/CFT supervision frequency is determined by taking into account the risk ratings provided to financial institutions, as well as the following factors, among others:

- Unusual increases in the number and threshold of transactions performed by financial entities
- Increases in the STRs or CTRs, among other types of reports
- Change of a financial institution's business line profile
- New financial products or new lines of business
- The level of compliance of financial institutions with their regulatory obligations (submission of AML/CFT program to the authority, and submission of reports in a timely manner, among others).

The AML/CFT supervision frequency is also subject to the follow-up of the corrective measures, including specific plans and timelines.

THE NETHERLANDS

Based on the perceived risks DNB allocates its supervisory resources through ongoing supervision and thematic reviews. This applies to both frequency and intensity of AML/CFT supervision. In the ongoing reviews DNB assigns more resources to institutions which have a higher risk profile (based on their size, activities, compliance history etc.). In the thematic reviews a specific subject/high risk area is examined for a selection of institutions.

UNITED KINGDOM

The UK's Financial Conduct Authority (FCA) categorises firms according to their money laundering risk:

- Firms in the highest band are covered by the Systematic AML Programme. The programme operates on a four-year, rolling cycle and each programme lasts several months.
- Firms in the second band are subject to a regular on-site inspection programme consisting of two or three day on-site visits every two years.
- Firms in the lower risk banks are visited on an events-driven basis or when they are part of a sample of a thematic review.

All firms can be subject to events-driven supervision and form part of thematic reviews.

UNITED STATES

The Federal Banking Agencies (FBAs) are required by law to conduct Bank Secrecy Act (BSA) examinations of insured depository institutions as part of their overall prudential supervisory function. Such reviews are conducted during regular examinations of their depository institutions, on a 12-18 month cycle, which is required by statute (12 U.S.C. §§ 1820(d) and 1784). Supervision and regulation of depository institutions for compliance with the BSA is conducted through a combination of on-site examinations and off-site reviews. FBA BSA examination policies and procedures are established in the Federal Financial Institutions Examination Council (FFIEC)'s *Bank Secrecy Act/Anti-Money Laundering Examination Manual.* FBAs are required to conduct required core examination procedures for assessing compliance with the BSA/AML compliance program, regulatory requirements and related topics. Expanded procedures for products, services, persons and entities are required depending on risk. Transaction testing is required during each examination regardless of the level and nature of risk present in the institution. For larger, more complex institutions, some FBAs maintain resident on-site examiners who provide continuous supervision of the institution and obtain at least quarterly updates on the institution's condition and risk assessment.

Examples of adjustment of the intensity of ML/TF supervision in line with the risks identified

AUSTRALIA

As described above, AUSTRAC uses a range of compliance techniques to assess the adequacy of RE Groups' policies, practices, systems and controls to meet the requirements of the AML/CTF Act, including:

- Low intensity or 'engagement' activities such as enrolment processes, mail-outs, e-newsletters, forums, workshops and the development and distribution of guidance materials.
- Moderate intensity or 'heightened' activities such as processes associated with the registration of remitters, behavioural assessments, desk reviews, themed reviews and transaction monitoring directed at specific behaviours of cohorts of reporting entities.
- High intensity or 'escalated' activities such as on-site assessments and a dedicated management approach. AUSTRAC tailors these activities to individual reporting entities. They are designed to have a direct impact on improving compliance outcomes.

Where an entity with high inherent ML/TF risk is assessed and shown to have inadequate policies, practices, systems and controls in place to address its compliance risk, these entities are prioritised for remediation and/or enforcement action.

Remediation processes are undertaken through issuing a compliance assessment report to an entity, which requires that entity to take specific actions to remedy non-compliance in specific timeframes. AUSTRAC then monitors the entity against those requirements.

GERMANY

BaFin has set up a risk-matrix for credit institutions (see above), and the intensity of supervision follows the risk classification of each institution. The main reasons for this approach are the necessity of concentrating on the highest risk areas and the need to allocate resources where they are most needed.

Differences in the levels of supervisory intensity include:

- On-site inspections always include sample testing. If lots of deficiencies appear in a certain field (e.g., customer identification process), this could lead to a so called "full-size check" (i.e. the identification process of all new customers acquired in the past 6 months is checked)

- Escalation steps can be taken in the follow-up procedure to on-site inspections. Institutions are dealt with individually, when specific events occur.

MEXICO

CNBV applies the methodology set forth in the Institutional Manual of Supervision, which contains a detailed description of all the procedures that must be held in order to assess significant activities (products and services) of higher risk that are determined by the offsite supervisory area, as well as the effectiveness of the mitigating actions implemented by the financial institution.

During the inspections, if the supervisor in charge determines that some risk mitigating actions that are not originally covered in the corresponding supervision program should be reviewed by virtue of having evidence that there is a weakness in their implementation or effectiveness, it has the faculties to conduct a deeper and more comprehensive review. E.g., if, based on a transaction report, a deficiency is detected in the automated system of the bank, the supervisor should proceed to verify the system in order to detect the actual cause of the deficiency.

THE NETHERLANDS

DNB will allocate its supervisory resources through ongoing supervision and thematic reviews. This applies to both frequency and intensity of AML/CFT supervision. DNB's approach to supervision makes a distinction between different regimes, for example low, neutral, high and urgent. Each institution is assigned to a specific supervision regime, based on an assessment of the chance that the identified risks within an institution could harm the supervisory objectives. The risk profile of the institution forms the basis for this. The supervision regimes set the tone for the risk mitigation activities which ranges from no substantial intervention to immediate intervention where all possible measures are used to mitigate the risk.

UNITED KINGDOM

The UK's Financial Conduct Authority (FCA) categorises firms according to their money laundering risk. This categorisation determines the intensity and frequency of AML/CFT supervision.

- Firms in the highest band are covered by the Systematic AML Programme (SAMLP). These firms are subject to the most intensive AML/CFT supervision, which consists of extensive interviews with key staff, including senior management, compliance and front office both in the UK and elsewhere, as well as detailed testing of the firm's AML/CFT systems and controls. A typical SAMLP lasts several months and is repeated every four years.
- Firms in the second band will be subject to a regular inspection programme, consisting of two or three day on-site visits every two years.
- Firms in the lower bands are mainly supervised through thematic reviews and event-driven reactive supervision. Thematic reviews typically involve an off-site assessment of the firm's policies and procedures and detailed

testing and interviews during an on-site visit that lasts between two and three days, depending on the size of the firm and the complexity of its operations. The intensity of event-driven supervision depends on the nature of the suspected breach.

Examples of different approaches to supervisory guidance

AUSTRALIA

An extensive range of guidance information on Australia's AML/CTF reporting obligations is available on the AUSTRAC website (www.austrac.gov.au), including:

Guidance Notes

AUSTRAC's guidance notes contain information regarding legislative provisions to provide assistance to reporting entities in meeting their obligations. Current guidance notes can be found on the AUSTRAC website at www.austrac.gov.au/guidance_notes.html.

Guides

AUSTRAC has released the following AML/CTF Guides, which are available at www.austrac.gov.au/guides.html:

- *AML/CTF compliance guide for pubs and clubs,* to assist hotels and clubs, which are licensed to operate electronic gaming machines, to meet their requirements under the AML/CTF Act and the AML/CTF Rules.
- *AML/CTF compliance guide for independent remittance dealers*, to assist providers of remittance services to determine whether they are required to register as an independent remittance dealer and how to complete the registration process.
- *AML/CTF compliance guide for bookmakers,* to assist bookmakers in understanding and meeting their obligations under the AML/CTF Act.
- *AUSTRAC business profile form explanatory guide,* to assist entities with using the AUSTRAC business profile form.

Guidelines

The AUSTRAC guidelines contain information related to aspects of the *Financial Transaction Reports Act* and cover aspects of the reporting requirements for cash dealers. For example, the *Significant Cash Transaction Reporting Guideline for Solicitors*, available at: www.austrac.gov.au/files/guideline_no6.pdf.

Compliance Guide

The *AUSTRAC Compliance Guide* consolidates a range of AUSTRAC guidance material. The guide outlines and explains the obligations under the AML/CTF Act, Rules and regulations and presents

examples on how they operate and assists reporting entities to design, develop and implement systems and controls necessary to mitigate the risks of money laundering and terrorism financing.

The current guide is at:
www.austrac.gov.au/businesses/obligations-and-compliance/austrac-compliance-guide

CANADA

FINTRAC has published a series of guidelines to ensure that reporting entities understand and comply with their legislative and regulatory AML/CFT obligations. All of FINTRAC's guidelines can be found at the following link: www.fintrac-canafe.gc.ca/publications/guide/guide-eng.asp FINTRAC has recently issued new guidance (Guideline 4) on how to implement a compliance regime, including in respect of the risk-based approach (see www.fintrac-canafe.gc.ca/publications/guide/Guide4/4-eng.asp).

OSFI, the Office of the Superintendent of Financial Institutions, has also issued guidance to assist reporting entities that are Federally-Regulated Financial Institutions to comply with applicable AML/CFT requirements (www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b8.aspx).

ITALY

The Bank of Italy regularly provides supervised entities with general feedback on controls activities and guidance on AML/CFT risks encountered in the exercise of supervisory tasks, as well as on AML/CFT measures recommended or requested at international level (i.e. FATF black list, UN sanctions). Guidance also contains instructions on the proper procedures for fulfilling anti-money laundering obligations and compliance with the rules.

In addition, the Italian FIU, in order to ease detection of STRs, produces guidance on anomalous conduct patterns of economic or financial behaviour that may be linked to money laundering or terrorist financing (e.g., conduct patterns regarding possible loan sharking issued in 2011, on ML risk of factoring issued in 2012, on gambling and betting issued in 2013). In some cases, the Italian FIU issues "alert notes" in order to foster the awareness of financial institutions on how certain financial instruments may be exploited for ML or TF purposes (e.g., alert note on pre-paid cards in 2012). Often this kind of guidance goes along with roundtables or (in) formal meetings with ML reporting officers in order to reduce wrong interpretation regarding STRs. Such contacts are used by reporting entities for implementing an efficient RBA approach and enhance internal procedures, due to the close relationship between STRs and overall AML and CFT policies.

THE NETHERLANDS

DNB has published several guidance documents to support institutions in implementing the AML/CFT requirements. After the off-site and on-site activities, the results are benchmarked to determine outliers and good practices. Institutions receive individual feedback and potentially enforcement actions follow. The industry also gets more generalized feedback (round table, seminar, (in) formal meetings) and overviews of good practices/guidance. The sectors are kept informed of the thematic examinations through an annual publication on the themes and regular updates through newsletters.

UNITED KINGDOM

Regulatory guidance

The Financial Conduct Authority (FCA) publishes regulatory guidance on a wide range of financial crime issues. This guidance sets out the FCA's expectations of firms' financial crime system and controls. It also includes questions firms can use to test the adequacy of their systems and controls and lists examples of good and poor practice observed during on-site visits to help firms understand how they can meet their financial crime obligations.

This guidance is not binding and the FCA will not presume that a firm's departure from this guidance constitutes a breach of its rules. But firms are expected to take note of what the guidance says and use it in a proportionate and risk-sensitive way to inform their own financial crime systems and controls.

The FCA regularly updates its guidance to take account of new findings and to clarify expectations in areas where weaknesses exist across many firms. All changes are subject to public consultation before being finalised. The FCA's guidance, **Financial crime: a guide for firms** is at http://media.fshandbook.info/Handbook/FC1_FCA_20140401.pdf

Industry guidance

When assessing the adequacy of firms' AML/CFT systems and controls, the FCA also has regard to the **Joint Money Laundering Steering Group (JMLSG)'s guidance**. This is guidance written by a group of UK financial services trade associations and sets out how firms can meet their legal and regulatory AML/CFT obligations. It is formally approved by the UK Government and referred to in the FCA's rulebook and guidance. The FCA liaises closely with the JMLSG during the revision of its guidance.

UNITED STATES

The FBAs issue guidance under their own supervisory authorities and jointly with the FIU (FinCEN) to their regulated financial institutions to communicate and clarify their supervisory expectations with respect to managing ML/TF risks and complying with AML/CFT regulations. As members of the Federal Financial Institutions Examination Council (FFIEC), the FBAs have issued the *Bank Secrecy Act/Anti-Money Laundering Examination Manual* that prescribes the procedures that FBA examiners are required to apply in conducting BSA exams. The procedures contained in BSA/AML Exam Manual address compliance with both FBA supervisory expectations as well as BSA regulatory requirements and ensure transparency in the examination process. It also ensures that exam procedures are comprehensive and applied consistently across all the institutions regulated by the FBAs. The FFIEC updates the Manual regularly to incorporate changes in regulations and supervisory expectations that reflect emerging ML/TF risks and any significant changes to existing ones.

ANNEX 2

BASEL CORE PRINCIPLES DESIGNATED BY THE FATF AS BEING RELEVANT TO AML/CFT SUPERVISION (R. 26)

Basel Core Principle	Element of Supervision
Principle 1	*Responsibilities, objectives and powers:* An effective system of banking supervision has clear responsibilities and objectives for each authority involved in the supervision of banks and banking groups. A suitable legal framework for banking supervision is in place to provide each responsible authority with the necessary legal powers to authorise banks, conduct ongoing supervision, address compliance with laws and undertake timely corrective actions to address safety and soundness concerns.
Principle 2	*Independence, accountability, resourcing and legal protection for supervisors:* The supervisor possesses operational independence, transparent processes, sound governance, budgetary processes that do not undermine autonomy and adequate resources, and is accountable for the discharge of its duties and use of its resources. The legal framework for banking supervision includes legal protection for the supervisor.
Principle 3	*Cooperation and collaboration:* Laws, regulations or other arrangements provide a framework for cooperation and collaboration with relevant domestic authorities and foreign supervisors. These arrangements reflect the need to protect confidential information.
Principle 5	*Licensing criteria:* The licensing authority has the power to set criteria and reject applications for establishments that do not meet the criteria. At a minimum, the licensing process consists of an assessment of the ownership structure and governance (including the fitness and propriety of Board members and senior management) of the bank and its wider group, and its strategic and operating plan, internal controls, risk management and projected financial condition (including capital base). Where the proposed owner or parent organisation is a foreign bank, the prior consent of its home supervisor is obtained.

Basel Core Principle	Element of Supervision
Principle 6	*Transfer of significant ownership:* The supervisor has the power to review, reject and impose prudential conditions on any proposals to transfer significant ownership or controlling interests held directly or indirectly in existing banks to other parties.
Principle 7	*Major acquisitions:* The supervisor has the power to approve or reject (or recommend to the responsible authority the approval or rejection of), and impose prudential conditions on, major acquisitions or investments by a bank, against prescribed criteria, including the establishment of cross-border operations, and to determine that corporate affiliations or structures do not expose the bank to undue risks or hinder effective supervision.
Principle 8	*Supervisory approach:* An effective system of banking supervision requires the supervisor to develop and maintain a forward-looking assessment of the risk profile of individual banks and banking groups, proportionate to their systemic importance; identify, assess and address risks emanating from banks and the banking system as a whole; have a framework in place for early intervention; and have plans in place, in partnership with other relevant authorities, to take action to resolve banks in an orderly manner if they become non-viable.
Principle 9	*Supervisory techniques and tools:* The supervisor uses an appropriate range of techniques and tools to implement the supervisory approach and deploys supervisory resources on a proportionate basis, taking into account the risk profile and systemic importance of banks.
Principle 11	*Corrective and sanctioning powers of supervisors:* The supervisor acts at an early stage to address unsafe and unsound practices or activities that could pose risks to banks or to the banking system. The supervisor has at its disposal an adequate range of supervisory tools to bring about timely corrective actions. This includes the ability to revoke the banking licence or to recommend its revocation.
Principle 12	*Consolidated supervision:* An essential element of banking supervision is that the supervisor supervises the banking group on a consolidated basis, adequately monitoring and, as appropriate, applying prudential standards to all aspects of the business conducted by the banking group worldwide.

Basel Core Principle	Element of Supervision
Principle 13	*Home-host relationships:* Home and host supervisors of cross-border banking groups share information and cooperate for effective supervision of the group and group entities, and effective handling of crisis situations. Supervisors require the local operations of foreign banks to be conducted to the same standards as those required of domestic banks.
Principle 14	*Corporate governance:* The supervisor determines that banks and banking groups have robust corporate governance policies and processes covering, for example, strategic direction, group and organisational structure, control environment, responsibilities of the banks' Boards and senior management, and compensation. These policies and processes are commensurate with the risk profile and systemic importance of the bank.
Principle 15	*Risk management process:* The supervisor determines that banks have a comprehensive risk management process (including effective Board and senior management oversight) to identify, measure, evaluate, monitor, report and control or mitigate all material risks on a timely basis and to assess the adequacy of their capital and liquidity in relation to their risk profile and market and macroeconomic conditions. This extends to development and review of contingency arrangements (including robust and credible recovery plans where warranted) that take into account the specific circumstances of the bank. The risk management process is commensurate with the risk profile and systemic importance of the bank.
Principle 26	*Internal control and audit:* The supervisor determines that banks have adequate internal control frameworks to establish and maintain a properly controlled operating environment for the conduct of their business taking into account their risk profile. These include clear arrangements for delegating authority and responsibility; separation of the functions that involve committing the bank, paying away its funds, and accounting for its assets and liabilities; reconciliation of these processes; safeguarding the bank's assets; and appropriate independent internal audit and compliance functions
Principle 29	*Abuse of financial services:* The supervisor determines that banks have adequate policies and processes, including strict customer due diligence rules to promote high ethical and professional standards in the financial sector and prevent the bank from being used, intentionally or unintentionally, for criminal activities.

BIBLIOGRAPHY

FATF (2012), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FATF Recommendations*, FATF, Paris, www.fatf-gafi.org/recommendations

FATF (2013a), *FATF Guidance National Money Laundering and Terrorist Financing Risk Assessment*, FATF, Paris, www.fatf-gafi.org/topics/methodsandtrends/documents/nationalmoneylaunderingandterroristfinancingriskassessment.html

FATF (2013b), *FATF Methodology for assessing with the FATF Recommendations and the effectiveness of AML/CFT systems,* FATF, Paris www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf

FATF (2013c), *FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22)*, FATF, Paris www.fatf-gafi.org/topics/fatfrecommendations/documents/peps-r12-r22.html

FATF (2013d), *Revised Guidance on AML/CFT and Financial Inclusion*, FATF, Paris www.fatf-gafi.org/topics/financialinclusion/documents/revisedguidanceonamlcftandfinancialinclusion.html

Financial Stability Board (2014), *Guidance on supervisory interaction with financial institutions on risk culture, A Framework for Assessing Risk Culture, Basel, Switzerland,* https://www.financialstabilityboard.org/publications/140407.pdf

BCBS (2005), *Compliance and the compliance function in banks*, BIS, Basel, Switzerland, www.bis.org/publ/bcbs113.pdf

BCBS (2010a), *Principles for enhancing corporate governance,* BIS, Basel, Switzerland, www.bis.org/publ/bcbs176.pdf

BCBS (2010b), *Good Practice Principles on Supervisory Colleges*, BIS, Basel, Switzerland, www.bis.org/publ/bcbs177.pdf

BCBS (2011), *Core Principles for Effective Banking Supervision,* Basel, Switzerland, www.bis.org/publ/bcbs213.pdf

BCBS (2014a), *Sound management of risks related to money laundering and financing of terrorism*, BIS, Basel, Switzerland www.bis.org/publ/bcbs275.pdf

BCBS (2014b) *Revised Good Practice Principles on Supervisory Colleges (Consultative document),* BIS, Basel, *Switzerland,* https://www.bis.org/publ/bcbs276.pdf

ESMA, EBA, EIOPA and Joint Committee of the European Supervisory authorities (2013), *Preliminary report on anti-money laundering and counter financing of terrorism Risk Based Supervision,* www.eba.europa.eu/documents/10180/16145/JC-2013-72+%28Report+on+Risk+Based+Supervision%29.pdf

